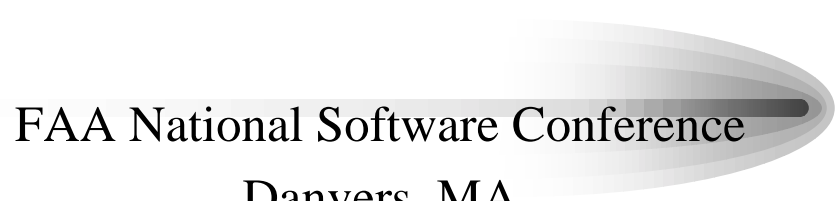


COTS Research
A Review of COTS Software in Airborne and CNS/ATM
systems

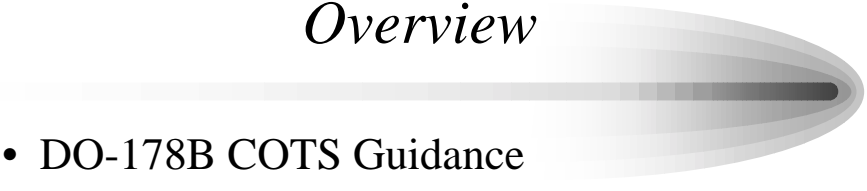


FAA National Software Conference
Danvers, MA
6-Jun-01

Jim Krodel
United Technologies Research Center
East Hartford, CT

1

Overview



- **DO-178B COTS Guidance**
 - “Software Consideration in Airborne Systems and Equipment Certification”
- **N8110.92 COTS Guidance**
 - “Guidance for Applying the RTCA/DO-178B level D Criteria to Previous Developed Software”
- **COTS Research Contract Findings**
- **DO-248B COTS Information**
 - “Final Report For Clarification of DO-178B”
- **DO-xxx COTS Information**
 - Guidelines for CNS/ATM Systems Software Integrity Assurance

2

In the limited time of this presentation I hope to brief the audience on the major COTS guidance or initiatives in both airborne and ground based systems.

Guidance from the FAA comes in the form of recognition that DO-178B will be the primary means of compliance for developing software in airborne systems. Also Notice 8110.92 provides further FAA guidance with regards to COTS in a level D system.

The FAA has also contracted out research work conducted by United Technologies Research Center that has demonstrated a need for further considerations when using COTS in an airborne system.

More recently RTCA special committee 190 has developed clarification of identified DO-178B guidance and produced DO-248 in consideration of this clarification text.

SC-190 has at this time obtained plenary consensus approval of proposed guidance with respect to Communications, Navigation, Surveillance (CNS) and Air Traffic Management (ATM). A portion of this document addresses COTS with respect to ground based systems and its content is summarized.



DO-178B COTS Definition

- Commercial off-the-shelf (COTS) software
Commercially available applications sold by vendors through public catalog listings. COTS software is not intended to be customized or enhanced. Contract-negotiated software developed for a specific application is not COTS software.
- Are there others? Yes, but we can work with this.

3

At a recent seminar at MIT in February, a COTS breakout session spent over 30 minutes trying to develop a clear definition of COTS. Indeed there is no one clear definition as the topic is rather subjective. Special Committee 167, which developed DO-178B, had several iterations of definitions before agreeing to this consensus definition.

DO-178B COTS Guidance

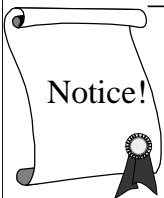
- In Brief
 - COTS needs to satisfy the objectives
 - Missing data needs to be augmented to satisfy the objectives
 - COTS use should be detailed in PSAC Additional Considerations section
 - Modifications to PDS
 - Reconsider SSA and SW level affects
 - Analysis to impact on reqs, architecture and re-verification of coupled software

4

DO-178B guidance on COTS is rather lightly addressed. Essentially COTS is viewed no differently from a safety point of view than any other software. However there are special considerations that must be given when using COTS. Missing data and the impact of COTS on the safety requirements are two major items that need to be considered. Because these special considerations may differ with different COTS packages, the PSAC must announce the use of COTS in the system and any alternate means of meeting the objectives of DO-178B with the COTS must be described.

N8110.92 Guidance

Guidance for Applying the RTCA/DO-178B level D Criteria to Previous Developed Software

- Formerly N8110.82 (Issued 3/29/1999)
 - Overview will be part of a break-out session
 - In brief for PDS
 - Level D software, does not need to meet DO-178B objectives A-2 4, 5, and 6 as they are inherently met.
 - These objectives mainly support the low level reqs and traceability guidance in DO178B.
- A graphic of a rolled-up scroll tied with a ribbon, with the word "Notice!" written on it.

Notice!
- The published notices can be viewed at the Web site <http://av-info.faa.gov/software/related.htm>

5

In lower software level systems, DO-178B has shown be too restrictive. The FAA recognizing this have published at this time Notice 8110.92 which essentially states that the lower level requirements and their traceability objectives, are inherently met for COTS at software level D.

Summary of FAA COTS Industry Study
Contract No. DTFA03-99-C-00030

- COTS Software AND Hardware
 - Study of current COTS industry
 - airborne, nuclear, medical, elevator
 - Study of Alternate Methods
 - wrappers, test & design techniques, etc.
 - Not a complete treatise, but a snapshot

Software **AND** **Hardware** ⁶

UTRC, in October of 1999, was contracted by the FAA to study the current status of the COTS industry in a variety of safety related domains. Methods to meeting the objectives from DO-178B with respect to COTS were also investigated. The report was submitted to the FAA in October of 2000 and is soon to be published.

The contract work included a study of both hardware and software aspects of COTS.



Background

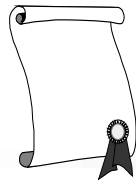
- Pressures of FAA certification applicants to reduce costs
 - Reuse
 - Commercially available components
- Assessment of COTS pedigree difficult
- Alternate methods being offered to verify components intent to DO-178B
 - Many alternate methods available

7

The Predicament Facing the FAA

The pressures to employ COTS software in airborne systems have created a new set of difficult questions for regulators. Aside from technical questions related to the safe integration of a COTS software product into the system, frequent difficulties are also encountered due to various competitive or management concerns. These concerns tend to interfere with access to records and information needed for product assessment. If the desired records and information are unavailable, the regulator (and developer) is then faced with either rejecting the COTS product for use in the system or must make a determination about the acceptability of the COTS software product. The basis for this acceptance criterion for the COTS product is different than those used for new developments, because of the lack of evidence in compliance to DO-178B's objectives.

Alternative methods of compliance is not only difficult, but relies on the regulator's ability to understand the alternate method and apply some amount of subjective evaluation that the methods meet the intent of DO-178B objectives or provides equivalent levels of confidence. It should be shown convincingly that alternative acceptance criteria provide confidence equivalent to that obtained from the processes applied to new developments.



COTS *The Issues*

- COTS (Commercial off the Shelf) software must meet the objectives of DO-178B
- Possible types of COTS
 - OS (Operating System)
 - Run time library
- The vendor may or may not have the necessary documentation / methodology to support certification
- If not then what?

8



Contract COTS Definition

- COTS - A product not developed within a company and in particular product development and test information is lacking.

9

As indicated before, a definition of COTS is rather difficult, but from a regulatory point of view, the definition can be viewed as stated above. The issue is that many COTS products lack some portion of development data that DO-178B requires.

Current Major COTS Components in Use in Safety Critical Systems

- Network Software
- Compiler Libraries
- Operating Systems
 - Several DO-178B specific discovered during study
 - Some have direct support for Safety Domain
 - Some provide plans and templates
 - Some provide certification assistance services

10

From the data obtained in this study, it appears there is only a small set of COTS components are seriously considered for COTS usage in safety-critical domains at this time. Most of these are of the type that enables the system to meet standards and open architectures.

Most vendors of COTS components used in the avionics industry that were contacted are not fully cognizant in DO-178B. Vendors made many inaccurate statements like "our software is FAA certified", or "our software meets DO-178B". Most of the vendors do not truly understand the software avionics domain guidelines in DO-178B. Indeed most do not even fully understand the different criticality levels of avionics software. Vendors will state that because their product was used in avionics equipment that it is fully DO-178B compliant even though their product has been used only to level D.

Operating Systems

There are several operating systems that have been used to some extent on certified avionics products including VRTX, LynxOS, PSOS, VxWorks and OSE to name a few. To better understand the issues, this research explored in more detail Enea's OSE and WindRiver's VxWorks operating systems. Note that the other operating systems listed also provide some level of safety consideration to their embedded product. No evaluation of capability between these vendors was made during this study and hence no judgments on their specific product are to be construed from this report.

Software Alternative Methods



- Monitors or Reasonableness Checks
- N-Version
- Wrappers
- Service History
- COTS Process Recognition
- Prior Product Certification
- Reverse Engineering
- Restriction of COTS Functionality
- Architectural Methods
 - Model Following
 - Graceful Degradation
 - Re-try fault recovery
 - not always good for real time safety critical systems
 - Dynamic Reconfiguration
 - not at all popular for real time safety critical systems

11

The list of alternative methods is certainly not exhaustive. And in fact it is not uncommon to have a combination of methods used to support one or more DO-178B objectives. No analysis was conducted to determine which method(s) could be applied to which objective(s). However DO-248B does provide some rationale in applying certain techniques above to certain DO-178B objectives.

The application of the list is also somewhat subjective. Some items on the list above may be viewed as not appropriate for an alternate method for meeting a DO-178B objective. For instance, an application of a wrapper in one application may be viewed as acceptable, but the particular use of a wrapper in another application may not.

A Deeper Look at Some Alternate Methods

- Reverse Engineering
 - Replacing Missing Documentation
- Service History
 - History data integrity establishment
 - Proper Service History Control Required
 - Data should be pertinent to Avionics domain
 - Some COTS vendors are motivated to suppress info
 - However
 - Allied fields of large numbers of installations are claimed by some to be a basis for acceptance.



12

Reverse Engineering

An approach to replacing missing data is to perform data reconstruction with methods such as reverse engineering. This can be a difficult task requiring as much effort as doing a new development and, even if accomplished, it is not clear that the reconstruction process was error-free. However, it may produce software life cycle data that can be reviewed or analyzed to satisfy the intent of the objectives of DO-178B/ED-12B, such as design structure, source code, or calling trees.

Replacing Missing Documentation

Considerable controversy rages about the acceptability of various approaches to replacing, reconstructing, or substituting for missing COTS product documentation. Some viewpoints focus on the question of applying engineering judgment to these and other assessment questions. In that light, engineering judgment should be applied carefully to specific, narrowly defined questions, and that the rationale for the judgment should be documented and able to withstand critical, external scrutiny.

Service History

Product service history is the utilization of previous in-service experience of the component. Previous use of a software product that is relevant to its intended application may constitute evidence of product integrity. The data integrity of the service history records needs to be validated. Details of the service history are needed, including information about the problem tracking process and software configuration management process.

COTS Operating Systems

- COTS O/S Vendors Seek DO-178B Lev A
 - An O/S based Software Hazard Analysis (SHA)
 - An O/S Plan for Software Aspects of Certification (PSAC)
 - Alternate Methods Considered for a COTS O/S
 - Rev Engr., partitioning, restriction of functionality
 - Compliance to Standards
 - COTS Integration
 - SQA & CM Concerns

13

At the time of this research effort, numerous operating system vendors were seeking to provide their commercial operating system (O/S) so that could it satisfy the intent of DO-178B, level A capability on a true off-the-shelf basis. Several of these vendors shared their approaches and expected deliverables with the principal investigator. In particular one vendor shared in detail their approach to developing a 'DO-178B-ready' operating system.

Some vendors were working directly with applicants on a particular aircraft system, while others hired experts to assist in developing a 'DO-178B ready' package. All of these efforts to make the COTS operating system 'DO-178B ready' were done with the COTS vendor and some form of the COTS developmental data was available. Because of this availability of data, the task of meeting the intent of DO-178B was somewhat simpler than trying to do the same without vendor cooperation.

Issues Concerning Usage of COTS with DO-178B

- Vendor & Applicant Business Relationship
- Problem Reports
- Unused / Unintended Functions
- Previous COTS Operational Environment
- Version Control
- New Releases
- Product & Process Examination

14

The Business Relationship Between the Vendor and Applicant

Under consideration is the fact that once a software component has been integrated into a safety critical application, its responsibility for performance and reliability is assumed, at least in part, by the applicant.

Problem Reports

For 'in-house' developed systems, problem reports from the deployed system require analysis for their effect on the overall system safety. Systems incorporating COTS exposes the safety of the system further and problem reports from the COTS vendor should be coordinated to allow visibility into problems that may have been previously masked.

Unused or Unintended Functions

Functions intended by the developer but not needed for the avionics application is one source of concern. Alternately, unplanned functions arising from the COTS design or implementation errors are another source of concern for COTS products.

COTS Previous Environment and Operational Profile


Proper evaluation of the COTS software requires a thorough understanding of the operational profile of the software's role in the system.

Version Control

It is important to understand that a COTS product could be so highly configurable that version information may require version control of individual sub-components of the COTS configured system.

Next Step of the Investigation

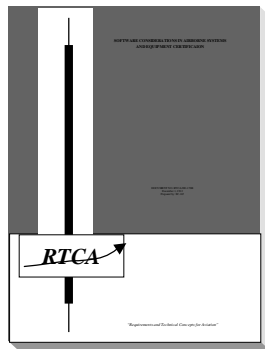
COTS Operating Systems



- Determine the various protection techniques
- Evaluate Time and Space Partitioning
- Select a COTS operating system
 - Suitable for avionics
 - Determine ability to support protection schemes
 - Identify particular characteristics of protection
 - Abstract findings to apply to O/S's in general

Summary of SC-190 DO-248A

Non-recognized Guidance relating to COTS



16

RTCA- Special Committee 190

Terms of Reference Summary

- Formed in 1996 by RTCA
- Joint with EUROCAE WG-52
 - Gain Consensus Clarification on DO-178B guidance
 - DO-248A
 - Resolve inconsistencies between DO-178B, and other relevant civil aviation standards.
 - Develop consensus position papers on those software issues which are beyond the scope of DO-178B
 - Develop guidance material based on DO-178B/ED-12B for Communication, Navigation and Surveillance (CNS) and Air Traffic Management (ATM) software
 - DO-xxx

17

DO-178B/ED-12B, “Software Considerations in Airborne Systems and Equipment Certification,” was published December 1, 1992, to provide recommendations for the production of software for airborne systems and equipment that performs its intended function with a level of confidence in safety that complies with airworthiness requirements. Since the date of publication, the aviation community has gained experience using DO-178B/ED-12B and has raised a number of questions regarding the document’s content and application. In order to address the questions of both the industry and certification authorities, the European Organization for Civil Aviation Equipment (EUROCAE) Working Group 52 (WG-52) and RTCA Special Committee 190 (SC-190) was formed in 1996.

The two committees worked jointly from 1996 until 2001, having ten joint meetings alternatively in Europe and United States.

The committee membership was composed of individuals coming from certification authorities and the aviation industry, including aircraft and engine manufacturers, equipment suppliers, software developers and consultants providing experience and expertise on software matters for both ground and airborne aspects. The total number of members of the committee was 331. This comprised 119 from Europe (including Russia), 209 from North America (USA and Canada), 2 from India and one from Australia.

Some SC-190 - Technology Issues

- **COTS**

- Shrink wrap, user-modifiable, user-selectable.
- What techniques can be used to accept COTS?
- System partitioning, requirements partitioning, partitioning integrity

- **CNS/ATM - Information Explosion**

- Growth of networking infrastructure is resulting in the clear airborne and ground systems division not as clear.
- Airborne and ground have different guidance on SW development.



18

SC-190 addressed many technical issues, two of which were directly related to COTS.

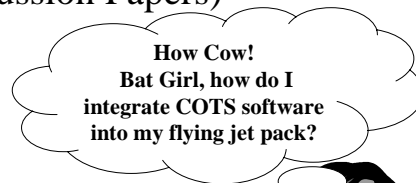
The COTS topic in and of itself was a subject that was tackled by the development sub-group of SC-190. Several FAQs and discussion papers were produced to address the issues presented to the team to solve.

The CNS/ATM community also had many COTS related issues as many of the CNS/ATM systems in place utilize a tremendous amount of COTS software.

DO-248A & COTS

- DO-248A
 - Not planned to be called out via FAA guidance
 - Format (FAQs and Discussion Papers)
 - COTS FAQs & DPs
 - FAQs: 4, 16, 17, 25, 26
 - DPs: 5, 10
- No New COTS Info in DO-248B
- Available at www.rtca.org

Full Text Available at www.rtca.org



DO-248A is one of the products of SC-190. The report will result in DO-248B sometime in late 2001, however between DO-248A and DO-248B there are no new FAQs or Discussion papers relating to COTS.

The Full Text can be purchased from RTCA. (www.rtca.org)

***FAQ #4:** Does DO-178B/ED-12B's definition of commercial off-the-shelf (COTS) software include COTS software designed for option-selectable software?*

DO-248A

- **Per DO-178B COTS Definition**
 - If the COTS product software is not changed, then it is COTS and treated as such.
 - Thus DO-178B COTS guidance should be met.
- **If it is option-selectable COTS**
 - Additional option-selectable guidance per DO-178B should be met. (Sect 2.4e, 5.4.3a, 6.4.43d)

Full Text Available at www.rtca.org

20

The Full Text can be purchased from RTCA. (www.rtca.org)

FAQ #16: What is the highest software level (per DO-178B/ED-12B) that can be attained for previously developed software (PDS)?
DO-248A

- Level A
- Must satisfy all objectives
- Allowed to use alternate means.



Full Text Available at www.rtca.org

21

The Full Text can be purchased from RTCA. (www.rtca.org)

***FAQ #17: What are the issues related to changing
previously developed software (PDS) versions from an
earlier baseline?***

DO-248A

- See 8110.89 (now 8110.78)
 - “Guidelines for changes in legacy systems using DO-178B”
- Same issue as any other software including
 - Change Impact to SSA and requirements.
 - Problem discovery via review of supplier’s PRs
 - Impact of re-verification and previous certification data package
 - And more..

Full Text Available at www.rtca.org

22

The Full Text can be purchased from RTCA. (www.rtca.org)

FAQ #25: Can architectural means be used to reduce the software level needed for the incorporation of previously developed software (PDS) in a system?

DO-248A

- Yes
 - Ref: ARP 4754 “Certification Considerations for Highly-Integrated or Complex Aircraft Systems”
 - Partitioning,
 - Safety monitoring, and
 - Multiple-version dissimilar software (with use of monitors, comparators, and polling) may be used for redundancy or backup
 - Other considerations
 - Assurance
 - Primary vs. Secondary
 - Common mode failures
 - Restriction of Functionality

Full Text Available at www.rtca.org

23

The Full Text can be purchased from RTCA. (www.rtca.org)

FAQ #26: Does the fulfillment of “independence of multiple-version dissimilar software” (DO-178B/ED-12B Section 12.3.3.1) supercede the independence requirements as defined in Annex A of DO-178B/ED-12B?

DO-248A

- Yes
- Per DO-178B we must show...
 - Different teams
 - Limited interaction in SW requirements, design and code definition

Golly Gee
Batman, I don't
know, let's read
DO-248A's
discussion paper!



Full Text Available at www.rtca.org

The Full Text can be purchased from RTCA. (www.rtca.org)

***DP #5: Application of Potential Alternative Methods of
Compliance for Previously Developed Software (PDS)
DO-248A***

- **Techniques**
 - Process Recognition
 - Prior Product Certification
 - Reverse Engineering
 - Restriction of Functionality
 - Product Service History
 - Formal Methods
 - Audits & Inspections
- **For each technique**
 - Description
 - Potential Achievements
 - Inputs
 - Limitations

For each table of objectives in Annex A of DO-178B, each of the above techniques are discussed as to their applicability to the method with respect to previously developed software.

Full Text Available at www.rtca.org

25

The Full Text can be purchased from RTCA. (www.rtca.org)

*DP #10: Considerations Addressed When Deciding to Use
Previously Developed Software (PDS)*
DO-248A

- Technical – System assurance level with respect to PDS, domain experience, CM, tools, etc.
- Business
 - Cost – acquisition, maintenance, licensing, code buyouts, escrow, etc.
 - Schedule – additional PDS tasks, make vs. buy decisions, time to market, etc.

Full Text Available at www.rtca.org

26

The Full Text can be purchased from RTCA. (www.rtca.org)

*Summary of SC-190 DO-xxx
Non-Recognized Guidance Relating to
CNS/ATM COTS*

- Based on DO-178B
 - Same objectives and need DO-178B to read DO-xxx
- Implemented via contract for the ground-based CNS/ATM developers
- Recognition of DO-xxx by the FAA very much unknown
 - Still very early
 - CAST review planned

27

DO-xxx is another product of SC-190. The report is under Final Review And Comment (FRAC) with RTCA and is expected to be approved by the RTCA Program Management Council sometime in late 2001.

The FAA at this time has no position as to the content of the document as it is still under review.

System Aspects Relating to COTS in CNS/ATM

DO-xxx

- COTS and Software Levels per System Safety Assessment
- Additional Considerations with respect to planning, acquisition, verification, etc.
- Risk mitigation possible via
 - People, Procedure, Equipment
 - Architecture: partitioning, redundancy, monitoring wrappers, etc.

The information here is preliminary and is subject to change

28

Note: The information here is preliminary and is subject to change. The Full Text can be purchased soon from RTCA. (www.rtca.org)

COTS Planning Process

- Objectives: *DO-xxx*
 - Plans for acquisition & integration, transition criteria, consistent plans
- Activities:
 - Assess plans with respect to product availability and associated life cycle data, etc.



The information here is preliminary and is subject to change

29

Note: The information here is preliminary and is subject to change. The Full Text can be purchased soon from RTCA. (www.rtca.org)

COTS Acquisition Process

DO-xxx

- Objectives:
 - Requirements satisfied, adequate COTS data, derived requirements defined, target compatibility
- Activities:
 - Assess COTS with respect to requirements, availability of lifecycle data, requirements needed to protect from unwanted COTS side affects (isolation), assess requirements imposed by COTS (initialization)

The information here is preliminary and is subject to change

30

Note: The information here is preliminary and is subject to change. The Full Text can be purchased soon from RTCA. (www.rtca.org)

COTS Verification Process

DO-xxx



- Objectives:
 - No new objectives
- Activities:
 - Reviews and requirements based testing of system requirements on COTS, verification of supplemental software (glue code, wrappers, etc.), verification of COTS integration, verification of any alternate methods used

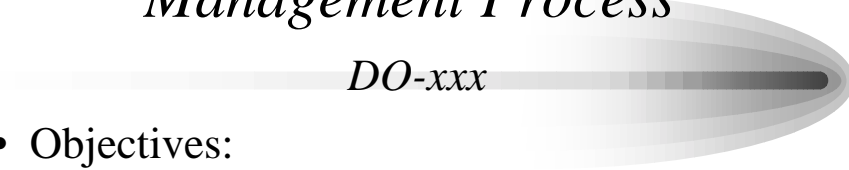
The information here is preliminary and is subject to change

31

Note: The information here is preliminary and is subject to change. The Full Text can be purchased soon from RTCA. (www.rtca.org)

COTS Configuration Management Process

DO-xxx



- Objectives:
 - Configuration and data items identified and archived, PR system, controlled COTS release
- Activities:
 - Method of identification from supplier, bi-directional problem reporting system

The information here is preliminary and is subject to change

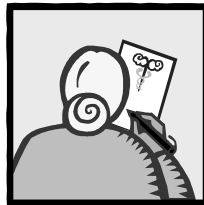
32

Note: The information here is preliminary and is subject to change. The Full Text can be purchased soon from RTCA. (www.rtca.org)

COTS Quality Assurance

DO-xxx

- Objectives:
 - No new objectives
- Activities:
 - Assure COTS specific activities are met



The information here is preliminary and is subject to change

33

Note: The information here is preliminary and is subject to change. The Full Text can be purchased soon from RTCA. (www.rtca.org)

COTS Software Specific Objectives

DO-xxx

- Tables are developed for planning, acquisition and CM related objectives very much like DO-178B
-
- *PLEASE NOTE: Assurance Levels for (CNS/ATM) are the same as Software Levels for (Airborne) except additional level for CNS/ATM between software level C & D.*

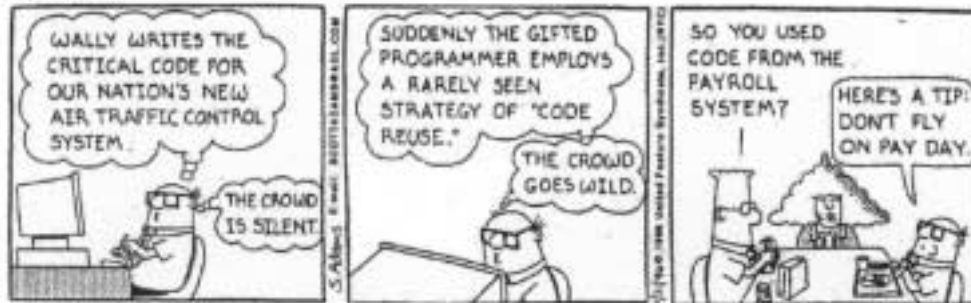
The information here is preliminary and is subject to change

34

Note: The information here is preliminary and is subject to change. The Full Text can be purchased soon from RTCA. (www.rtca.org)

WEDNESDAY, January 31, 1996

Dilbert



Dilbert's Perspective on Software Reuse

Source: Scott Adams from someone's masters thesis

35

Many thanks to Scott Adams and Leanna Rierson's master's thesis for the most appropriate cartoon above.

Summary



- **DO-178B COTS Guidance**
 - “Software Consideration in Airborne Systems and Equipment Certification”
- **N8110.92 COTS Guidance**
 - “Guidance for Applying the RTCA/DO-178B level D Criteria to Previous Developed Software”
- **COTS Research Contract Findings**
- **DO-248B COTS Information**
 - “Final Report For Clarification of DO-178B”
- **DO-xxx COTS Information**
 - “Guidelines for CNS/ATM Systems Software Integrity Assurance”

36

Guidance from the FAA comes in the form of recognition that DO-178B will be the primary means of compliance for developing software in airborne systems. Also Notice 8110.992 provides further FAA guidance with regards to COTS in a level D system.

The FAA has also contracted out research work conducted by United Technologies Research Center that has demonstrated a need for further considerations when using COTS in an airborne system.

More recently RTCA special committee 190 has developed clarification of identified DO-178B guidance and produced DO-248 in consideration of this clarification text.

SC-190 has at this time obtain plenary consensus approval of proposed guidance with respect to Communications, Navigation, Surveillance (CNS) and Air Traffic Management (ATM). A portion of this document addresses COTS with respect to ground based systems and its content is summarized.

Questions & Answers?



37